Decision Notice 066/2023

Cyber-attacks: neither confirm nor deny

Applicant: The Applicant

Public authority: Chief Constable of the Police Service of Scotland

Case Ref: 202100439

Scottish Information Commissioner

Summary

Police Scotland were asked about incidents in which their online resources had been hacked or compromised. Police Scotland refused to confirm or deny whether the information existed or was held by them. The Commissioner accepted that it was in the public interest for Police Scotland not to reveal whether the information existed or was held.

Relevant statutory provisions

Freedom of Information (Scotland) Act 2002 (FOISA) sections 1(1) and (6) (General entitlement); 2(1)(b) (Effect of exemptions); 18(1) (Further provision as respects responses to request); 35(1)(a) (Law enforcement)

The full text of each of the statutory provisions cited above is reproduced in Appendix 1 to this decision. The Appendix forms part of this decision.

Background

1. On 24 November 2020, the Applicant made a request for information to the Chief Constable of the Police Service of Scotland (Police Scotland). The Applicant requested

   any detail on incidents in which Police Scotland websites, databases, social media accounts - including accounts of officers - or other online resources - or resources connected to the internet - have been hacked or compromised? This should include any attack on these resources and any incidents in which passwords were compromised or accounts, websites or internet-connected resources taken control of by an unauthorised agent.

2. He asked for any incidents within the last three years or another "feasible" timescale.

3. Police Scotland responded on 23 December 2020. They refused to confirm or deny whether the information sought existed or was held by Police Scotland. They cited section 18(1) in conjunction with 35(1)(a) (Law enforcement) of FOISA.

4. On 28 December 2020, the Applicant wrote to Police Scotland requesting a review of their decision. He commented that other public bodies had released information on attacks on their services. He referred to the Scottish Environment Protection Agency (SEPA) having disclosed substantial information[1] about an attack on its services in December 2020, including the date of the attack and the services affected. The Applicant also commented that the Scottish Government had fully answered a similar request. In his view, if other public bodies, including the Scottish Government, could disclose information on attacks, or lack of attacks, then Police Scotland should be able to do the same.

5. The Applicant suggested that any information which could lead to attack opportunities or confirm the success of an attack could simply be redacted from the data. He considered that a blanket ban on releasing any information was not proportionate and that it was in the public interest for the public to know if their data had been compromised.

6. Police Scotland notified the Applicant of the outcome of their review on 12 February 2021. They continued to refuse to confirm or deny whether the information existed or was held by them. They stated that redaction was not appropriate in this case: any confirmation of attack

[1] https://www.sepa.org.uk/about-us/cyber-attack/

would provide those intent on causing harm to police systems with additional information in order to do so. Confirming that information existed could also encourage others to engage in similar activities. On the other hand, confirming no information existed could have a similar effect as Police Scotland may be seen as a "challenge" or potential target. It would also confirm to someone, if they had managed successfully to attack the system, that their efforts had gone undetected and could encourage them to continue or "leverage their positions".

7. Police Scotland considered that they were in a unique position. both in terms of the sensitivity of the information they held and processed, and in terms of the effect on the efficiency of the police service and on the risk to public safety which confirming the existence of this information would have.

8. On 7 April 2021, the Applicant wrote to the Commissioner, applying for a decision in terms of section 47(1) of FOISA, as he was dissatisfied with the outcome of Police Scotland's review.

Investigation

9. The application was accepted as valid. The Commissioner confirmed that the Applicant made a request for information to a Scottish public authority and asked the authority to review its response to that request before applying to him for a decision.

10. Section 49(3)(a) of FOISA requires the Commissioner to give public authorities an opportunity to provide comments on an application. Police Scotland were invited to comment on this application and to answer specific questions about why section 18 of FOISA applied to the Applicant's request.

Commissioner's analysis and findings

11. In coming to a decision on this matter, the Commissioner considered all of the relevant submissions, or parts of submissions, made to him by both the Applicant and Police Scotland. He is satisfied that no matter of relevance has been overlooked.

Section 18 (Neither confirm nor deny)

12. Police Scotland refused to confirm or deny whether they held any information falling within the scope of the Applicant's request.

13. Section 18(1) of FOISA allows public authorities to refuse to confirm or deny whether they hold information in the following limited circumstances:

    (i) a request has been made to the authority for information which may or may not be held by it;

    (ii) if the information existed and was held by the authority (and it need not be), it could give a refusal notice under section 16(1) of FOISA, on the basis that the information was exempt information by virtue of any of the exemptions in sections 28 to 35, 38, 39(1) or 41 of FOISA; and

    (iii) the authority considers that to reveal whether the information exists or is held by it would be contrary to the public interest test.

14. Where a public authority has chosen to rely on section 18(1), the Commissioner must therefore establish whether the authority is justified in stating that to reveal whether the information exists or is held would be contrary to the public interest. He must also establish

whether, if the information existed and was held by the public authority, the authority would be justified in refusing to disclose the information by virtue of any of the exemptions listed in section 18(1) and cited by the authority.

15. It is not sufficient to claim that one or more of the relevant exemptions applies. Section 18(1) makes it clear that the authority must be able to give a refusal notice under section 16(1), on the basis that any relevant information, if it existed and were held, would be exempt information under one or more of the listed exemptions. Where the exemption(s) is/are subject to the public interest test in section 2(1)(b) of FOISA, the authority must also be able to satisfy the Commissioner that the public interest in maintaining the exemption(s) outweighs any public interest there would be in disclosing any relevant information it held.

16. In any case where section 18(1) is under consideration, the Commissioner must ensure that his decision notice does not confirm one way or the other whether the information requested actually exists or is held by the authority.

Section 35(1)(a) (Prejudice to prevention or detection of crime)

17. In this case, Police Scotland submitted that if they held any information falling within the scope of the Applicant's request, it would be exempt from disclosure by virtue of the exemption in section 35(1)(a) of FOISA.

18. In order for the exemption in section 35(1)(a) of FOISA to apply, the Commissioner has to be satisfied that disclosure of the information would, or would be likely to, prejudice substantially the prevention or detection of crime (section 35(1)(a)). There is no definition in FOISA of what is deemed to be substantial prejudice, but the Commissioner considers the authority would have to identify harm of real and demonstrable significance. The harm would also have to be at least likely, and therefore more than simply a remote possibility.

19. As the Commissioner's guidance[2] on the section 35(1)(a) exemption highlights, the term "prevention or detection of crime" is wide ranging, encompassing any action taken to anticipate and prevent crime, or to establish the identity and secure prosecution of persons suspected of being responsible for crime. This could mean activities in relation to a specific (anticipated) crime or wider strategies for crime reduction and detection.

Submissions from Police Scotland

20. Police Scotland commented that it was not exceptional for individuals to enquire about hacking attempts made against them. Nonetheless, Police Scotland were concerned that confirming whether they held information could provide attack opportunities. This could be used by a hostile party to plan and execute an attack on Police Scotland's systems or to indicate that such an attack had gone undetected. Such attacks could take the form of data theft, denial of service or other deliberate disruptions. This would reduce the ability of Police Scotland to undertake relevant activities.

21. Police Scotland stated that, while other public bodies may have disclosed information in response to similar requests, Police Scotland were in a unique position in terms of the sensitivity of the information they hold and process and in terms of the effect disclosure would have on the efficiency of the Police service and subsequent risk to public safety.

---

[2] https://www.itspublicknowledge.info/sites/default/files/2022-04/BriefingSection35LawEnforcement.pdf

Submissions from the Applicant

22. The Applicant believed that the information could be disclosed, assuming it existed and were held, as he did not accept that harm would occur if the information (if held) were disclosed under FOISA.

23. As noted above, the Applicant referred to examples of other Scottish public authorities disclosing information and believed Police Scotland should be able to do the same.

24. He had also suggested that any information which could lead to attack opportunities or confirm the success of an attack could simply be redacted.

The Commissioner's conclusions

25. When considering whether a public authority has the right neither to confirm nor deny whether information exists or is held, the Commissioner must consider the information which could theoretically be held within the scope of the request.

26. In this case, the request is widely drawn. It covers a relatively wide timescale: a three-year period. It refers to a number of possible subjects of the request, i.e. Police Scotland websites, databases, social media accounts (including accounts of officers), "other online resources - or resources connected to the internet" that have been hacked or compromised.

27. Given the breadth of the request, the Commissioner accepts that, if held, the disclosure of some of the information theoretically covered by this request would, or would be likely to, cause substantial prejudice to the prevention or detection of crime. He goes on to consider the public interest test in section 2(1)(b) in relation to this set of information below.

28. It is clear that cybercrime is becoming ever more prevalent. Indeed, Police Scotland's Cyber Strategy 2020[3] recognises that: *In recent years there has been a steady trend of cyber enabled and cyber dependant crime increasing in Scotland and the wider UK.*

29. While Police Scotland consider themselves to be different from other public authorities (and no doubt they are in many respects), many public bodies, such as SEPA and the NHS, also process sensitive data and have placed information into the public domain about cyber-attacks.

30. Police Scotland referred to press reports about the NHS having suffered a number of unsophisticated cyber-attacks due to a lack of basic IT security. In Police Scotland's view, this can only demonstrate that any information Police Scotland release into the public domain could be used to their detriment by further encouraging hackers to attempt to breach their systems.

31. Given the breadth of the request, the Commissioner accepts that it includes information which, if held, would be exempt information by virtue of section 35(1)(a) of FOISA.

32. The Commissioner is now required to go on to consider the public interest test in section 2(1)(b) in relation to this set of information or whether, in terms of section 18(1) of FOISA, revealing whether the information exists or is held would be contrary to the public interest.

---

[3] cyber-strategy.pdf (scotland.police.uk)

The public interest test - section 2(1)(b)

33. As the Commissioner has found that the exemption in section 35(1)(a) would apply to the information covered by the request, if held, he is required to consider the public interest test in section 2(1)(b) of FOISA. He has therefore considered whether, in all the circumstances of the case, the public interest in disclosing the information would be outweighed by the public interest in maintaining the exemption in section 35(1)(a) of FOISA.

34. The "public interest" is not defined in FOISA, but has been described as "something which is of serious concern and benefit to the public", not merely something of individual interest. The "public interest" does not mean "of interest to the public" but "in the interest of the public", i.e. disclosure must serve the interests of the public.

Submissions from Police Scotland

35. Police Scotland recognised that there were various factors in favour of disclosing information, if held, even if disclosure would, or would be likely to, cause substantial prejudice to the prevention or detect of crime. These included Police Scotland's accountability for public funds in terms of the cost to the public purse and the public interest in informing the public of any vulnerabilities within their systems and the subsequent safety of their data.

36. However, there were also factors which would favour maintaining the exemption in section 35(1)(a) and which would outweigh these considerations: disclosing such information, if held, would have an adverse effect on the efficiency of Police Scotland and would provide those intent on disrupting police activities with enough information to plan and execute a targeted attack or indicate to them that such an attack had been detected or gone unnoticed. In addition, where systems were compromised, there was also the potential for sensitive information such as personal data, security information and other data to be made public.

Submissions from the Applicant

37. The Applicant considered that, if the information were held, the public interest would lie in its disclosure as there was a public interest in the public knowing if their data had been compromised.

The Commissioner's conclusions on the public interest test in section 2(1)(b)

38. The Commissioner has considered carefully the submissions as to where the public interest might lie here. It is worth remembering that he is considering here whether the public interest in disclosing information which (if held) would, or would be likely to, prejudice substantially the prevention or detection of crime would be outweighed by the public interest in maintaining the exemption.

39. In this case, he accepts there would be a clear public interest in ensuring that Police Scotland are able to continue to investigate crime and protect the public. He accepts that there would be a clear public interest in the security of Police Scotland's IT systems and the security of the information held.

40. The Commissioner also acknowledges the general public interest in transparency and accountability. He accepts that disclosure of such information (were it held) would allow public scrutiny of the extent of security of Police Scotland and allow an assessment of whether the systems used by Police Scotland are secure and effective.

41. On balance, the Commissioner is satisfied that, in relation to this set of information, if the information existed and were held by Police Scotland, the public interest in maintaining the

exemption in section 35(1)(a) would outweigh any public interest in disclosure of the information. The Commissioner recognises the vital importance of allowing Police Scotland to fulfil their functions in a complete and effective manner.

42. The Commissioner is therefore satisfied that, if information falling within the scope of the request existed and was held, Police Scotland could give a refusal notice under section 16(1) on the basis that the information was exempt information under section 35(1)(a) of FOISA.

The public interest test – section 18(1)

43. Having accepted that Police Scotland could give a refusal notice under section 16(1) of FOISA, the Commissioner must go on to consider whether Police Scotland were entitled to conclude that it would be contrary to the public interest to reveal whether the information existed or was held.

Submissions from the Applicant

44. The Applicant considered that it was in the public interest to reveal whether information existed or was held. He stated that he did not understand how confirmation of an attack or confirmation of non-attack could provide future attack opportunities, giving examples of other public bodies which had released information.

45. He also commented that there were mechanisms that required or encouraged the reporting of cyber-attacks, for example the UK Financial Conduct authority.

Submissions from Police Scotland

46. Police Scotland submitted that any indication of whether there have been and if so the number of attacks on Police Scotland's systems can only be detrimental to their ability to maintain security: were they to confirm whether any systems had been compromised, then this would tell attackers that they have vulnerabilities that they can then try to exploit. If Police Scotland state that they have not had any incidents then this would motivate attackers "to try for their self-esteem and credibility within their hacktivist group".

47. Police Scotland consider that police organisations are very different to the Scottish Government and other departments in that they process especially sensitive information that can be a threat to life if exposed; therefore, they need to be more careful about what is disclosed.

48. Police Scotland highlighted that the Current National threat level is "Substantial" and the direct threat to police employees from extremists and terrorists is also at "Substantial" so they have a duty of care to their staff for their safety. Police Scotland stated that to release this type of information "could motivate an attack that could potentially compromise staff personal details and allow extremists to attack them."

49. As noted above, Police Scotland referred to press reports about the NHS having suffered a number of unsophisticated cyber-attacks due to a lack of basic IT security. In Police Scotland's view, this can only demonstrate that any information released into the public domain could be used to the detriment of the organisation by further encouraging hackers to attempt to breach their systems.

50. Police Scotland re-iterated that the threat of cyber-attack on any organisation is real and current. They referred[4] to the cyber-attack on SEPA on Christmas Eve 2020, and that the source of the attack was suspected to have been perpetrated by international serious organised criminals utilising sophisticated 'Ransomware' tactics and techniques. They referred to the war in Ukraine, which has seen Russia threaten cyber-attacks on the UK, and concerns about Russian cyber-attacks on the UK. The aim of these attacks may be to merely hinder day to day life or it may be to steal information. Police Scotland commented that it is not possible to say what the intention of an attack would be. Therefore, in their view, it cannot be in the public interest to put any information into the public domain that could assist crime groups in achieving their goal.

51. Police Scotland also referred to a reported instance of a cyberattack on the Police Federation website in March 2019[5] and to other specific cyber risks: were Police Scotland to confirm or deny their status, they could also be targeted.

The Commissioner's conclusions

52. The Commissioner has very carefully considered the arguments presented by both parties. The test he must consider is (having already concluded that certain information, if it existed and were held, would be exempt from disclosure) whether revealing if that information exists or held would be contrary to the public interest.

53. The Commissioner accepts that disclosing information on specific attacks, etc. (if they had occurred) would not be in the public interest for the reasons set out by Police Scotland. However, the question the Commissioner is considering here is not whether specific information (if held) should be disclosed, simply whether it would be contrary to the public interest for Police Scotland to confirm or deny whether they hold any information covered by the information request.

54. As noted elsewhere, there is information in the public domain about incidents of hacking or unauthorised access to public authority resources, both UK and Scottish. Police Scotland supplied an instance with respect to the Police Federation. There are reports in the public domain of individuals having been prosecuted of such offences.

55. However, the Commissioner accepts Police Scotland's arguments about the importance of its cyber-security. Such security is vital to all Scottish public authorities, but the security of an authority such as Police Scotland – given its function - is of the highest importance and must therefore attract a weighty public interest. The Commissioner acknowledges that the Applicant himself is here espousing a similar public interest, albeit one that favours transparency of just such cyber resilience.

56. Each case will be assessed by the Commissioner on its own merits. On balance, the Commissioner is satisfied, in this case, that it would be contrary to the public interest for Police Scotland to reveal whether the information requested exists or is held by it. Consequently, the Commissioner concludes that Police Scotland were entitled to refuse to confirm or deny, in line with section 18(1) of FOISA, whether they held the information requested, or whether that information existed.

---

[4] police-scotland-cyber-attack-response-debrief.pdf

[5] https://www.polfed.org/news/latest-news/2019/cyber-attacks-impact-federation-it/

Decision

The Commissioner finds that the Chief Constable of the Police Service of Scotland complied with Part 1 of the Freedom of Information (Scotland) Act 2002 in responding to the information request made by the Applicant.

Appeal

Should either the Applicant or Police Scotland wish to appeal against this decision, they have the right to appeal to the Court of Session on a point of law only. Any such appeal must be made within 42 days after the date of intimation of this decision.

Daren Fitzhenry
Scottish Information Commissioner

5 July 2023

Appendix 1: Relevant statutory provisions

Freedom of Information (Scotland) Act 2002

1 General entitlement

(1) A person who requests information from a Scottish public authority which holds it is entitled to be given it by the authority.

…

(6) This section is subject to sections 2, 9, 12 and 14.

2 Effect of exemptions

(1) To information which is exempt information by virtue of any provision of Part 2, section 1 applies only to the extent that –

…

(b) in all the circumstances of the case, the public interest in disclosing the information is not outweighed by that in maintaining the exemption.

…

18 Further provision as respects responses to request

(1) Where, if information existed and was held by a Scottish public authority, the authority could give a refusal notice under section 16(1) on the basis that the information was exempt information by virtue of any of sections 28 to 35, 38, 39(1) or 41 but the authority considers that to reveal whether the information exists or is so held would be contrary to the public interest, it may (whether or not the information does exist and is held by it) give the applicant a refusal notice by virtue of this section.

…

35 Law enforcement

(1) Information is exempt information if its disclosure under this Act would, or would be likely to, prejudice substantially-

(a) the prevention or detection of crime;

…